RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: PART1-T09

Improving Immunity to Phishing Attacks

Dr. Lili Ana
Head of Security Shared Services, Trellix | Author
lilianaauthor/ @Dr_LiliAna_

Trellix
RSAC 2025 Conference

Phishing as a Service (PhaaS)

In 2025 around 50% of credential attacks will make use of PhaaS

Mind of the CISO Research: Decoding the GenAI Impact

500 security executives interviewed across North America

of CISOs agree GenAI has made them contemplate their future and career choice as a CISO

of CISOs lack confidence in their organization's workforce to successfully identify cyberattacks incorporating GenAI

of CISOs do not have a plan in place to educate employees on advanced GenAI attacks

RSAC 2025 Conference

Improving Immunity to Phishing Attacks

Conceptual Framework

Identifying what employees need to identify phishing attacks

Addressing Cybersecurity Gaps

Knowledge

- Factual
- Procedural
- Conceptual
- Metacognitive

Motivation

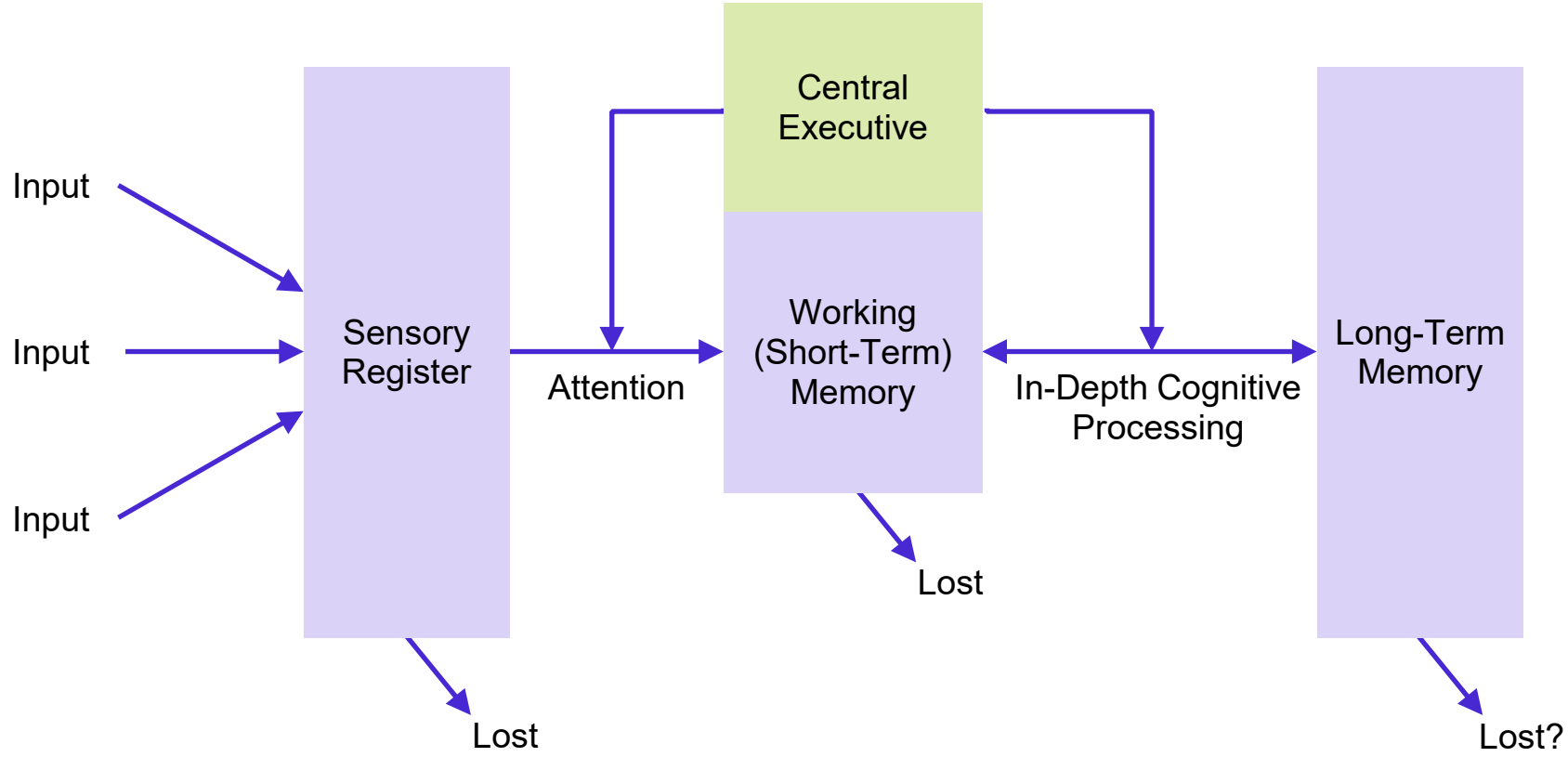
- Self-Efficacy
- Value

Organizational Influences

- Training
- Communication
- Culture

The Science of Memory and Learning

- Why employees don't retain certain information
- Why paying attention matters



Insights from Employee Interviews

"Most training when it comes to phishing, I don't feel is very relevant"

"It depends on your audience, right? Gen Ys and Gen Zs love gamification"

"I think if there were negative consequences maybe I would be a little more cautious"

"My confidence is going lower, as threat actors start using Generative AI to prep phishing emails"

"It'd be nice to know what common phishing scams we would potentially see so that we would be more aware"

RSAC 2025 Conference

Building a Training Program

Educational Framework

		Outcome, Critical Behaviors, or Methods	Metrics	Data Collection Methods	Timing
Level 4 Results	**External Outcomes**	Zero data incidents are reported to regulatory agencies	Number of violations reported	Emails	
	Internal Outcomes	Employees achieve under 5% phishing click rates	Amount of individuals who click on phishing simulations	Phishing Simulations	
Level 3 Behavior	**Critical Behaviors**	Employees read information security newsletters	Number of page visits and visitors	Newsletter Clicks	Monthly
	Driver - Reinforcing	Verbal warning from information security			First Infraction
	Driver - Encouraging	Employees receive recognition in newsletter for not clicking on phishing simulation template			Quarterly
	Driver - Rewarding	Employees receive reward points for completing educational program			Annual
	Driver - Monitoring	Employee compliance to policies and procedures			Ongoing

Educational Framework (continued)

Level 2 Learning	Learning Goals	Learn key concepts to identify advanced phishing attacks			
	Evaluation - Declarative Knowledge “I know it”	Knowledge checks			During Training
	Evaluation - Procedural Skills “I can do it right now”	Reporting phishing emails			After Training
	Evaluation - Attitude “I believe this is worthwhile”	Discussions about training value and rationale			Before, During, and After Training
	Evaluation - Confidence “I think I can do it on the job”	Peer check-ins			During and After
	Evaluation - Commitment “I will do it on the job”	Signed policy			After Onboarding
Level 1 Reaction	Engagement	Attendance			Orientation
	Relevance	Job roles are defined with manager as it relates to interacting with data			Before Orientation
	Employee Satisfaction	Survey			After Orientation

Enhancing Phishing Simulations

Discovering employee susceptibility to phishing attacks using LLMs and GenAI

Audience

Understanding the administrator's challenges and needs and simplifying the user experience by identifying phishing attacks circulating the region, industry, and environment

Training

AI-driven pre-built templates with relevant content to design role-based, rank-based, and risk-based training that is automated, customized, and personalized

Analytics

In-depth and actionable data and metrics to identify vulnerable team members and drive improvements in behavioral modifications

RSAC 2025 Conference

Communicating for Impact

Leveraging Communication Channels

What's a channel?

A method to host and direct the flow of information

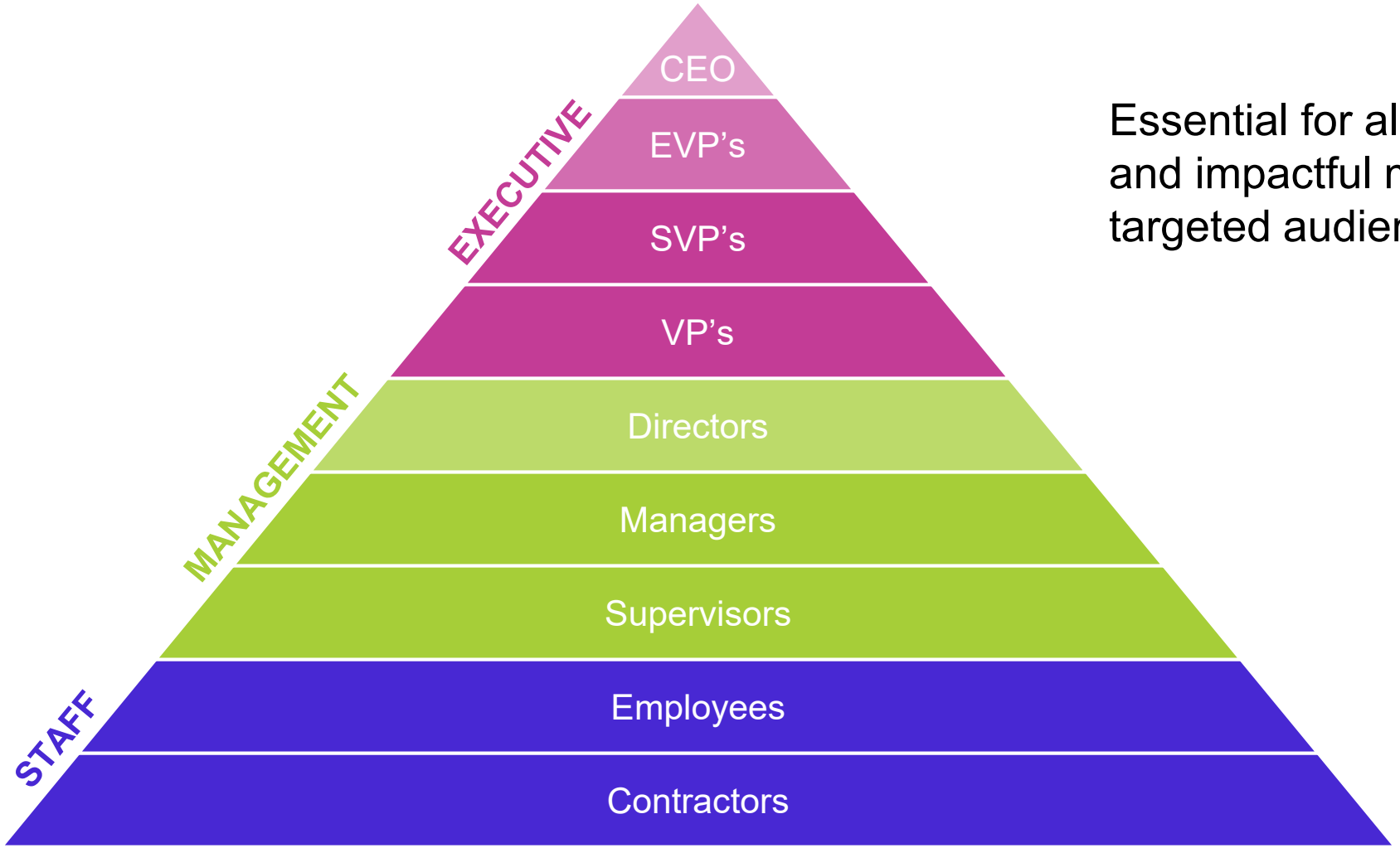
How to measure success?

Track user behavior, participation levels, and communication methods

Why does this matter?

An integrated approach to messaging engages employees

Segmenting Populations

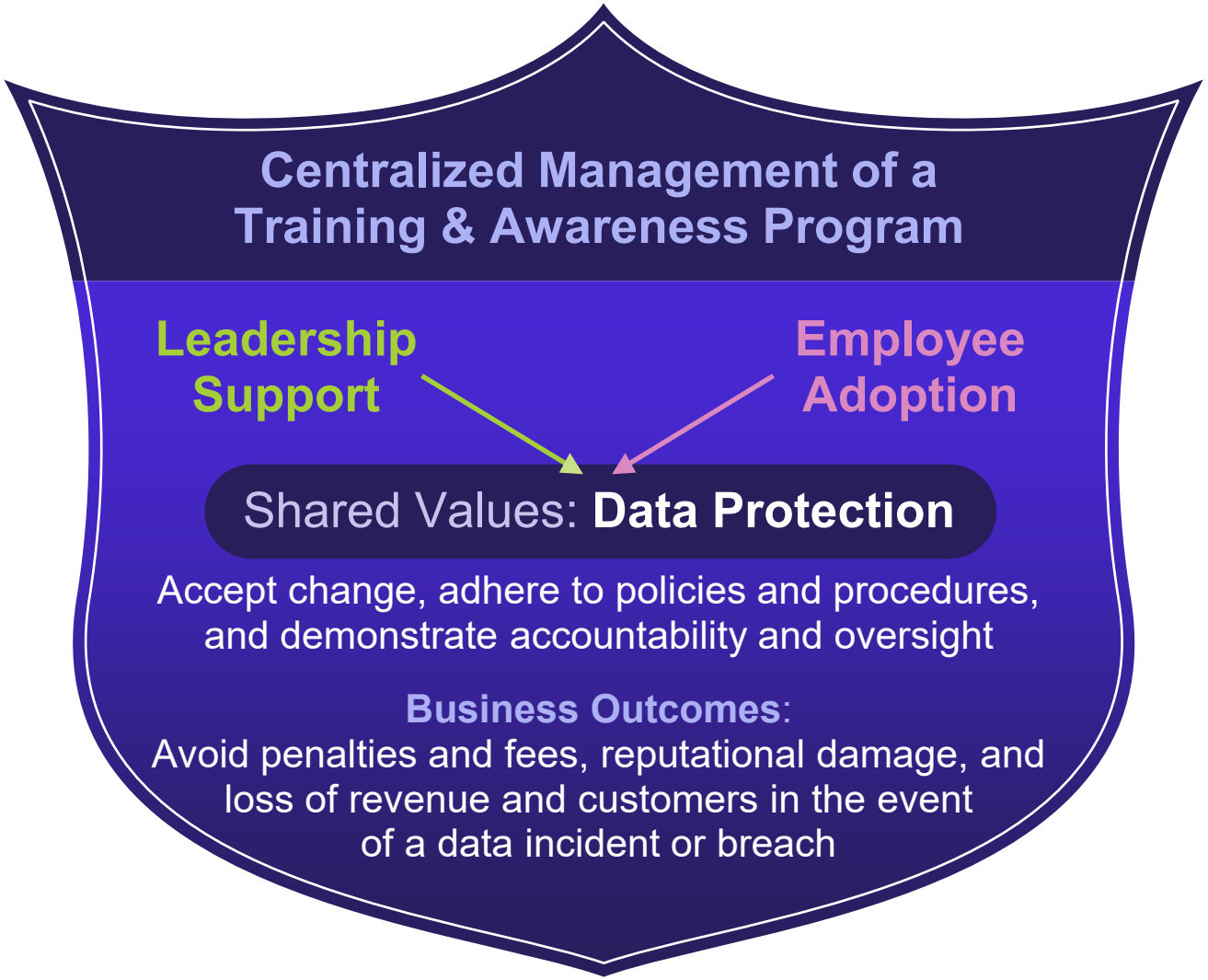


Essential for aligning appropriate and impactful messaging to targeted audiences.

RSAC 2025 Conference

A Cultural Model to Embrace Security Awareness

Cultural Model

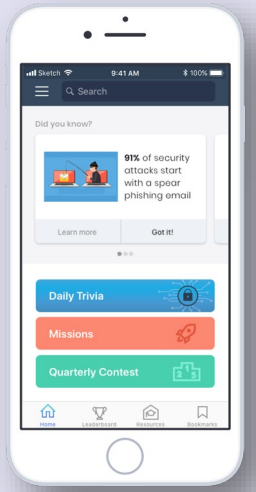

Centralized Management of a Training & Awareness Program
Leadership Support
Employee Adoption
Shared Values: Data Protection
Accept change, adhere to policies and procedures, and demonstrate accountability and oversight
Business Outcomes:
Avoid penalties and fees, reputational damage, and loss of revenue and customers in the event of a data incident or breach

Constantly **promoting** and **measuring** the value of a security awareness program supports buy-in across employees and leadership.

How to “promote”

Create a brand, use gamification, and excitement to drive employee engagement

HOW THE GRINCH
TRIED TO STEAL DATA
INFOSEC
What is Phishing?
Phishing is a type of digital fraud
If you aren't vigilant, these attackers can trick you into handing over your personal data such as usernames, passwords, and other sensitive information. You can find these destructive scams in Emails, Social Media, Instant Messaging, and SMS/Text Messaging.
Avoid Phishing Scams
Use these 3 tips to help you identify red flags:
1 Follow Your Instincts: Phishing emails most commonly contain spelling errors, urgent requests for action, or requests for sensitive data.
2 Think Before You Link: Inspect links by hovering over them and seeing where they are taking you. Only click on trustworthy/familiar URLs.
3 Report Message Button: Use your report message button, located at the top right corner of your email, if you aren't sure or if you see the red flags from above.
Learn more about The Report Message Button by clicking on the job aid button below:
Job Aid
Spot Phishing Scams
Click the button below to watch a quick video on what to do to protect yourself from phishing attempts:
Watch Now!
Interested in visiting the Information Security Website to learn more about Phishing? Click the button below:
InfoSec Website



How to “measure”

Compare phishing simulation results to drive leadership engagement

Phishing Simulation Division Scorecard

Division	Executives Caught VPs & Above	Clicks compared to Total Division Population	Replies to Hacker	Users Entering Credentials Compared to Q4	Repeat Offenders Compared to Q4 phishing simulation and legitimate phishing clicks in Q4	Click Rate Compared to Q4	Report Button Rate Compared to Q4
A	6	443 of 2,745	13	14 2	65, 47 2	16.1% 7.6%	10.3% 14.2%
B	10	776 of 3,315	18	179 0	115, 94 3	23.4% 9.9%	8.2% 11.8%
C	1	74 of 665	0	30 0	4, 10 0	11.1% 6.4%	1.5% 13.9%

Q1 Performance QQ

Click Rate: 16.2% ↑ (9%)
- 1,915 Associates Clicked Links

Report Button Rate: 9.9% ↓ (4%)
- 1,169 Associates Reported Phishing

Repeat Offenders: ↑
- 217 Associates Repeating Behaviors Compared to 160 Associates in Q4

Risk Levels

Low: < Rate | Medium: <1+ Rate | High: >1+ Rate

Key Takeaways

Apply Lessons Learned

Actionable steps to implement an effective training and awareness program

Establish	• Define business and security objectives • Conduct an audit to identify gaps • Develop a security brand, cultural model, and training framework
Engage	• Cultivate trusted partnerships with stakeholders • Segment audiences, tailor messaging, and leverage channels • Identify champions and ambassadors
Evaluate	• Establish key performance indicators and metrics • Monitor behaviors, track progress, and report performance • Capture insights to evaluate program effectiveness

RSAC | 2025 Conference

Many Voices.
One Community.

Thank You!

Dr. Lili Ana
Head of Security Shared Services, Trellix | Author
lilianaauthor/ @Dr_LiliAna_